Lab 4 - Password Cracking

EECS 4481 4.0 Computer Security Lab, Winter 2015

Due: Feb 11th, 2015, 11:59pm.

Format: Individual

Learning Objective: In this lab, you will recover passwords using two different techniques: dictionary attack and precomputation attack. Recovering a password, known as password cracking, can be a devastating attack, especially since most users will reuse the same password on different systems. Also, physical access to a machine represents an important opportunity for attackers to compromise the system and gain access. This will be explored by using bootable media to compromise an operating system.

1 Forced Entry with Bootable Media

The Ultimate Boot CD (UBCD) provides an extensive set of tools and operating systems that can be booted from external media. The UBCD is a completely separate operating system and runs independently of any hard drives. The UBCD file system is completely on the CD. Booting under UBCD, you can mount and modify the files on your original Linux/Windows drive.

Using UBCD break into your Linux system. That is, as a user without root access you will have booted the machine and altered its configuration so that you can gain root access when it is restarted. For example, try to modify the `/etc/shadow` file.

Report: Provide the steps you followed to break into Linux.

Using UBCD change the administrator password of Windows XP. That is, as a user without administrator access, boot the machine and alter its password so that you can gain administrator access when it is restarted.

Report: Provide the steps you followed to break into Windows, as well as recommendations for countermeasures.

2 Password Cracking (Windows)

1. Boot the Windows XP workstation in your VMWare environment.

2. You should find a shortcut to `ophcrack` on your desktop. Double click to run it.

3. Use `ophcrack` to crack the passwords on the Windows XP workstation (i.e. the local passwords). The tutorial under Help is thorough and will guide you through the use of the tool.

4. Create some new user accounts with different passwords and attempt to crack them. Attempt to create a password of less than 15 characters that cannot be cracked.

Report: Discuss what kind of passwords can `ophcrack` crack and what it can not. How can you employ it to crack non-local passwords?

3 Password Cracking (Windows)

1. Review the documentation included with version 6 of `pwdump`.

2. Run the `PwDump.exe` command to extract your Windows system's user password hashes. Be sure to use your system's hostname instead of localhost. Write the output to a file and then copy the file to the Linux workstation.

3. Use `John the Ripper` to execute a dictionary attack against the Windows password files. In order to do this, you may use your Linux system's built-in spellcheck dictionary, located at `/usr/share/dict/words`, or you may download a larger dictionary from some other source. Be sure to observe the dictionary format requirements.

4. On the Windows workstation, study an alternative to `pwdump` called `fgdump`.

Report: Compare the two password cracking methods for Windows you experimented with. Also, explain the difference between `pwdump` and `fgdump`.

4 Network Password Attack

You have discovered that some users connect to Windows Server using telnet. This means that some crucial user information is sent in clear text. Create an attack which collects user names and passwords.

Report: Explain the attack and show gathered user names and passwords.